# IDS in WSN Based on Spy Node & Neighboring Voting Scheme (SNNVS)

**Anupriya**

M.tech(cse) 4th sem Mehrishi Ved vyas engineering college yamunanagar

***Abstract:*** **WSN mechanisms cannot at present ensure that an attack will not be launched. For example, using a compromised node an adversary could perform an attack acting as a legitimate node of the network to acquire all the information. Such attacks are known as internal attacks. Therefore, it is important to protect the wireless sensor network from internal attacks, which is the purpose of this work. The algorithm for transport layer attack has been developed in this thesis which also works for the minimization of energy consumption. We have tested the algorithm for sink hole attack mainly but it can also works for other attacks like black hole, worm hole attack too.**

***Keywords*****: WSN, Security, Energy, Protocol**

## I. INTRODUCTION

Typically, WSNs contain a large number of sensor nodes, which are densely and randomly deployed in the field under study as shown in figure 1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to a collection point called a Sink. Data are forwarded to the Sink through a multihop wireless architecture as shown in figure1. Once the collected data reach the sink, it has to route them to the task manager, where the appropriate decisions can be made. The sink may communicate with the task manage rnode via Internet or satellite. The purpose of deploying a WSN is to report relevant data for processing which enables right decision making at the right moment. There are three types of reporting: event-driven, on-demand and continuous monitoring. In the event-driven reporting, the sensor network is tailored to detect the occurrence of a pre-specified type of event within the sensor field. Once this event occurs, the reporting task is initiated and the related information is forwarded to the Sink. Thus communication is triggered by the event occurrence and only nodes within the event area become sources of communication. The most famous detection based applications are: fire, food detection and alarms. In the on-demand reporting, communication is initiated by the Sink, and sensor nodes end their data in response to an explicit request. The important corresponding application is an inventory control system.

One of the key features of a WSN is its multihop distributed operations, which add more complexity in terms of security attack detection and prevention. In a multihop distributed environment, it is very difficult to locate attackers or malicious nodes. Many security attack detection and prevention mechanisms are designed for WSNs; however most of the existing solutions are capable of handling only a few security attacks.

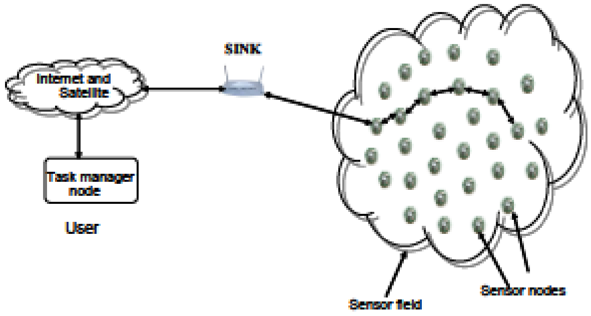

Figure 1: WSN design.

For example, most secure routing protocols are designed to counter few security attacks. Similarly new media access mechanisms are designed to handle hidden-node problem or selfishness. Encryption mechanisms are designed to protect data against passive attacks. Hence, one can say that there is a need to design mechanisms that are capable enough of detecting and preventing multiple security attacks in WSNs. An Intrusion Detection System (IDS) is one possible solution to it. An intrusion is basically any sort of unlawful activity which is carried out by attackers to harm network resources or sensor nodes. An IDS is a mechanism to detect such unlawful or malicious activities. The primary functions of IDS are to monitor users' activities and network behavior at different layers. A single perfect defense is neither feasible nor possible in wireless networks, as there always exist some architectural weaknesses, software bugs, or design flaws which maybe compromised by intruders. The best practice to secure wireless networks is to implement multiline of security mechanisms; that is why IDS is more critical in wireless networks. It is viewed as a passive defense, as it is not intended to prevent attacks; instead it alerts network administrators about possible attacks well in time to stop or reduce the impact of the attack. The accuracy of intrusion detection is generally measured in terms of false positives (false alarms)and false negatives (attacks not detected), where the IDSs attempt to minimize both these terms. There are two important classes of IDSs. One is known as signature-based IDS, where the signatures of different security attacks are maintained in a database. This kind of IDS is effective against well-known security attacks. However, new attacks are difficult to be detected as their signatures would not be present in the database. The second type is anomaly-based IDS. This kind is effective to detect new attacks; however it sometimes misses to detect well-known security attacks. The reason is that anomaly-based IDSs do not maintain any database, but they continuously monitor traffic patterns or system activities.IDS can operate in many modes, for example, standalone operation and cooperative cluster based operation. A standalone IDS operates on every node to detect unwanted activities. Cooperative cluster based IDS are mostly distributed in nature in which every node monitors its neighbors and surrounding nodes activities and operation; in case of any malicious activity detection, the cluster head is informed. Broadly speaking, IDS has three main components as:

i. Monitoring component is used for local events monitoring as well as neighbors monitoring. This component mostly monitors traffic patterns, internal events, and resource utilization.

ii. Analysis and detection module is the main component which is based on modeling algorithm. Network operations, behavior, and activities are analyzed, and decisions are made to declare them as malicious or not.

iii. Alarm component is a response generating component, which generates an alarming case of detection of an intrusion.

WSN suffers from various attacks by anomaly nodes. These nodes are stated as intruders which can alter the message passed to base station. As WSN is used in various applications like in emergency data transfer, military applications, surveillance etc. so requirement of accurate information is necessary, but if any intruder is active in the network and unidentified then false information can be transferred to head which may lead to dire consequences. So it is necessary to detect these anomaly nodes. For this many problems are faced WSN is a resource constrained and energy constrained network. So there is always scarcity of resources and battery in sensor nodes so conventional IDS can't be used for WSN. Many IDS presented by researchers are limited to only network layer due to which many types of attacks by intruders may go unidentified. So detection scheme should be such that it can analyze the anomaly node at each OSI layer so that attacking probability decreases or in other words cross layer detection scheme should be tried. Crossover detection has a problem of using different IDS at each layer which consumes more energy and resources too. So a generalize algorithm for almost all type of attacks should be proposed.

In our work we will establish the WSN network unsupervised learning as it don't require prior training. Since sensor nodes are resource constrained so we will put a mobile spy in WSN which will take data from every sensor node. Detection mechanism has to be deployed on each node which consumes battery of node, rather than we will deploy this only on spy node as it will have the information of every sensor node. Neighboring Voting mechanism will be followed for intruder detection in spy node and results will be shown in form of false alarms in case of different attacks in network.

## II. PROPOSED ALGORITHM

In WSN all nodes transfer their data to base station, it takes a lot of energy, so a hierarchical strategy of data transmission is followed in which clusters are formed and nodes are assigned to the nearest cluster head conditionally it must be farthest with other nodes in other clusters. K-means clustering follows this mechanism. Security issue is always a concern in WSN and since it is not following any particular infrastructure, it is more vulnerable to sink hole attack which occurs at its network layer and either alter the information or open path for worm hole attack. For this a security mechanism on the basis of voting scheme is developed in which neighboring nodes take part to clear the doubt of malicious node. it increases the true detection of sink hole node which is discussed in results section of this paper. If detection mechanism is processed on node end, then energy consumption in sensor nodes will be high which is calculated by following method:

The energy consumed in transmission and reception of message is calculated by [6]:

$$E_{consumed} = (E_{rx} \times Data\ Packet) + (Eth \times Data\ Packet) \tag{2.1}$$

If alarm is raised by node itself then energy consumption can be formulated as:

$$E_{consumed} = (E_{rx} \times Data\ Packet) + (Eth \times Data\ Packet) + (Eprocess \times Data\ Packet) \tag{2.2}$$

Equation 2.1 and 2.2 clearly shows the difference between energy consumed. If alarm process is not run on the ode then energy requirement will be less. So to avoid running detection mechanism on nodes, a spy node is used which will keep moving in the network and collect data form cluster heads at pre allocated polling points. This spy node is free from any battery constraint. It will follow a round path from base station to base station. The detection mechanism will be run on spy node. it collects data from cluster head and check whether any doubt is raised or not, if raised then it will follow voting mechanism and raises alarm to base station. The travel path for spy node is already designed in previous step. In WSN when any node transmits data then it also add its ID along with destination ID and data. This is used as a loop hole

IJRRA

in proposed work to detect the sinkhole. When sink hole gets the data and transmits it to head after altering it, it has to add its ID also. This all table of data sent from nodes to head is passed to spy node which can easily check the last hope node ID. If multiple nodes send data through compromised node to cluster head then in their routing table malicious node ID will be in last hope node ID to cluster head. If the occurrence of this same ID is more than two times, then that node is confirmed as malicious node and base station removes that from network.

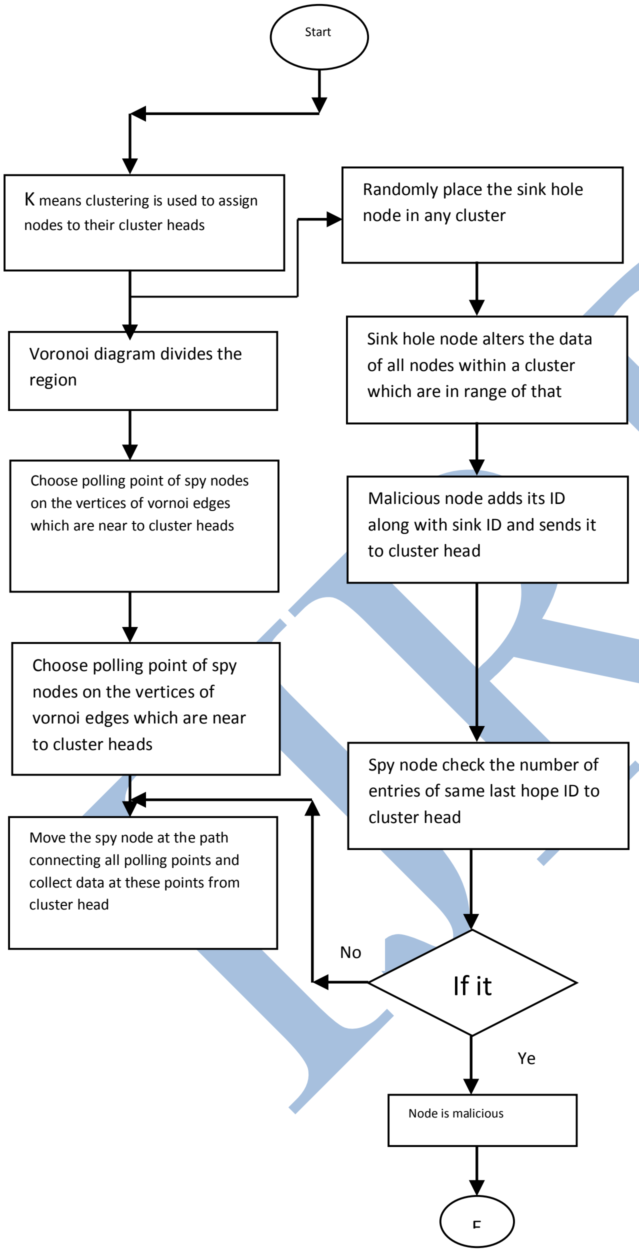
Start
K means clustering is used to assign nodes to their cluster heads
Randomly place the sink hole node in any cluster
Voronoi diagram divides the region
Sink hole node alters the data of all nodes within a cluster which are in range of that
Choose polling point of spy nodes on the vertices of vornoi edges which are near to cluster heads
Malicious node adds its ID along with sink ID and sends it to cluster head
Choose polling point of spy nodes on the vertices of vornoi edges which are near to cluster heads
Spy node check the number of entries of same last hope ID to cluster head
Move the spy node at the path connecting all polling points and collect data at these points from cluster head
No
If it
Ye
Node is malicious
E

Figure 2.2: Flow Chart of Proposed Work

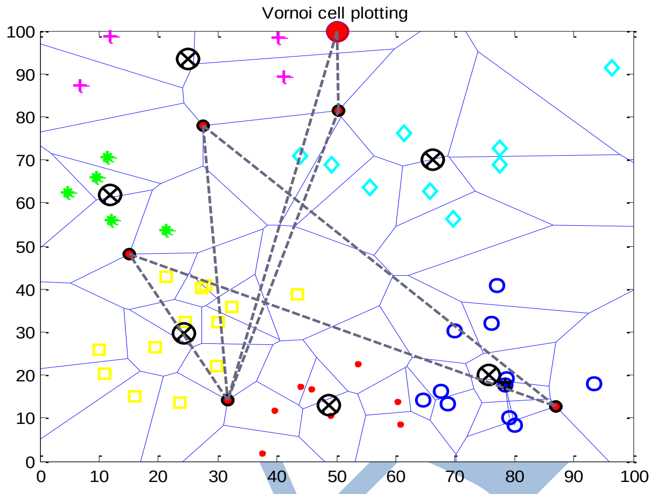

Figure 2.1: Malicious node detection by spy node

Figure 2.1 shows the spy node moving on pre assigned path and when it reaches to vulnerable cluster head, a communication link has been setup with that and detection algorithms on spy node decides whether any node is malicious or not. The flow chart for the movement of spy node is shown in figure 2.2.

## III. RESULTS

As discussed we have used clustering for the initial nodes placement and k means clustering approach is used because of simple and effective implementation. Initially we have checked our algorithm for 50 nodes and later nodes number is varied and simulation time too. Because measuring simulation time in MATLAB may actually differ from real world so we have renamed this term as number of iterations. For 50 nodes clustering, decision of the number of cluster heads is equally important. For this we have used silhouette plot which tells node is assigned to wrong cluster if plot is on negative axis as shown in figure 3.1 and 3.2.

The nodes placement in network affects the security and energy consumption, if nodes are placed at a far distance from base station, then they consumes a lot of energy in transmission and intruder can also easily affect whole network before detection. So k means clustering solve this problem. In our algorithm, trade off between energy and security are developed by moving a spy node in the network as discussed in previous section.

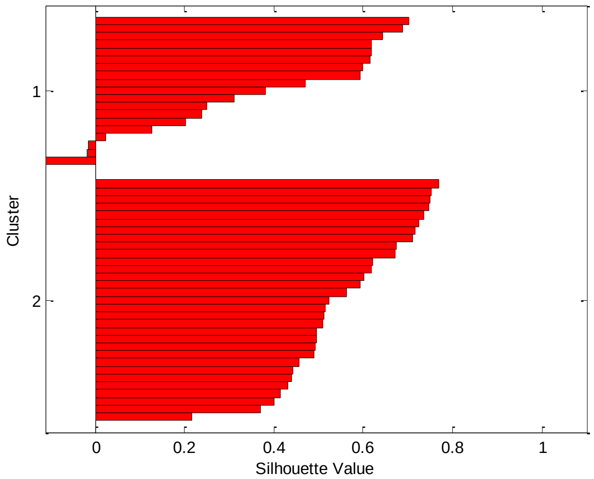

Figure 3.1: silhouette plot for 50 nodes with two cluster heads

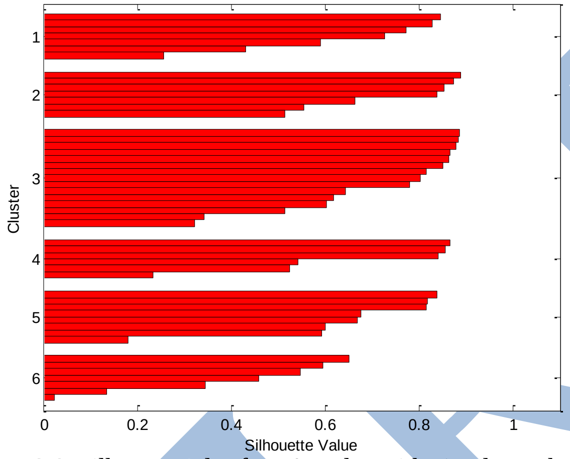

Figure3.2: silhouette plot for 50 nodes with six cluster heads

We have considered the energy constraint and calculated energy in each transmission and reception of message through a sensor node who takes part in communication. Parameters considered in this thesis are tabulated in table 3.1.

Table 3.1: Parameters' values considered for the simulation

| | |
|---|---|
| Nodes | [50 100 150 200 250 300 350 ] |
| Geographical area | 100*100 square meter |
| Energy consumed in reception | 50 nJ |
| Energy consumed in Transmission | 50 nJ |
| Data packet length | 10Kb |
| Energy consumed in detection process | 5nJ* |
| Packet size for sending alarm to base station | 5Kb |
| Transmission range of sensor nodes | 10 meter |
| Number of iteartions | [5,10,15,20,25,30] |

When nodes in the network increases, the nodes affected by intruder also increases. This is shown in figure3.3.

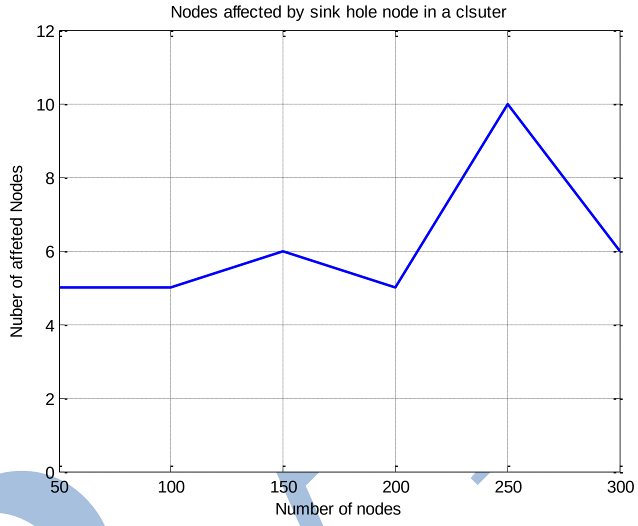

Figure 3.3: Number of affected nodes by sink hole

Maximum nodes in a cluster are affected when density of nodes is 250 in 100*100 geographical area. We have considered single sink hole node which is placed randomly in any cluster every time when new iteration is started. Results have been checked for 50 to 350 nodes and for each number of nodes system is executed from 5 to 30 times, a total of 630 times system have been executed. Figure 3.4 shows the total number of true detection of Sybil nodes. For 50 number of nodes our algorithm skip the detection of sink hole upto a large extent with maximum of 60 % detection in 15 iterations. But as the nodes in the network increased from 50 to 100, a sudden change in locating the sink hole is observed. True detection reached upto 100% in many iterations.

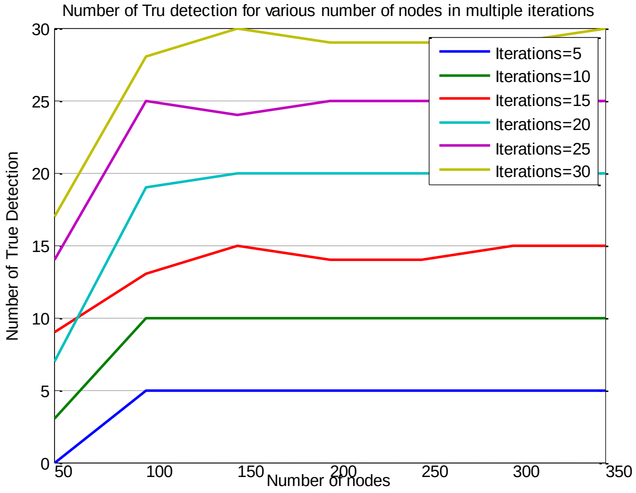

Figure 3.4: total number of true detection for multiple nodes and iterations

For further increase in number of nodes, promising results are visible. The average of percentage of true detection is shown in figure 3.5. It shows that for large number of nodes established in a particular geographical area, sink hole location is in between 0.88-0.92, which is quite impressive.

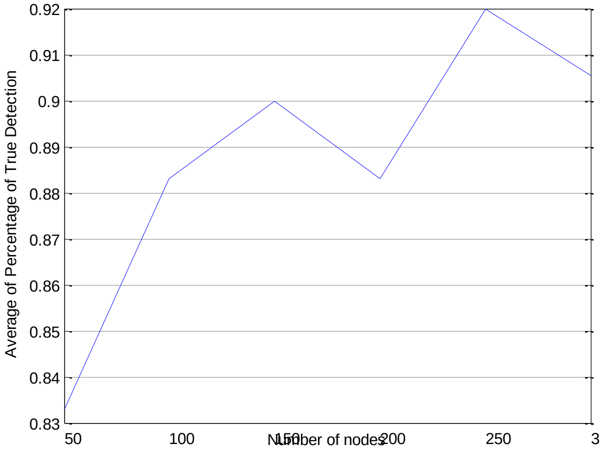

Figure 3.5: Average number of true detection for multiple iterations

our algorithm reduces the energy consumption along with enhanced security. For this a spy node runs in the network and intruder detection mechanism runs on spy node. Energy consumption for process is calculated using method discussed in equations 2.2 and 3.3. In this energy calculation, only nodes which are affected by malicious nodes are considered as rest nodes are not taking part in transmission in our case. A comparison of energy consumption for multiple sensor nodes is show in figure 3.6.

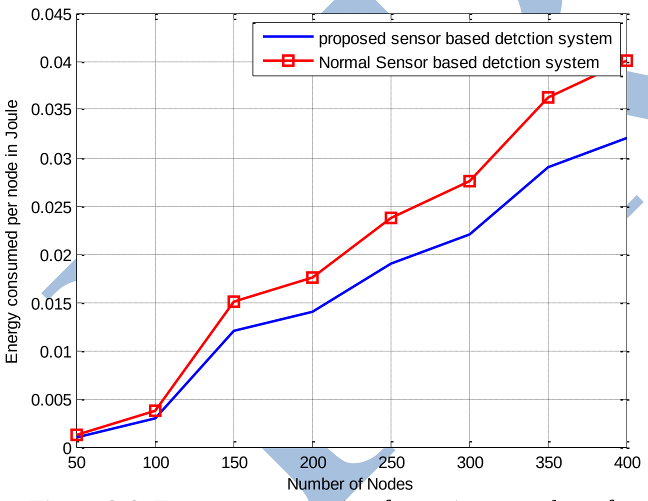

Figure 3.6: Energy consumption for various number of nodes

As nodes are increasing, energy consumption difference is also increasing because of detection mechanism consumption. Since more density of nodes become reason of more nodes affected by intruder. So detection algorithm will be executed by every affected node and this consumes more energy. That's why the difference between both curve in above figure is increasing with density of nodes.

## IV. CONCLUSION

This work is step forward to development of algorithm which can enhance security and reduce energy consumption at nodes. We have studied about wireless sensor network and their attacks with challenges to mitigate them in the very beginning of this work. Since all algorithms can't be avoided by a single universal algorithm, so it makes a clear picture of type of attack to be considered in our work. Sink hole attack occurs at network layer, so detection mechanism will also execute at that layer. Our mechanism reduces the energy consumption and this difference increases with number of nodes in the network. It has been proved that proposed algorithm is also performing well for security too. The detection of intruder is ranging between 0.88-0.92 for various numbers of nodes which is a good factor for true detection.

## REFERENCES

[1]. G.N. Purohit, "implementation of energy efficient coverage aware routing protocol for wireless sensor network using genetic algorithm."IJFCST, Vol.5, No.1, January 2015.

[2]. Umamakeswari Arumugam, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks." Journal of Sensors, Article ID 203814.

[3]. Mahdi Shahedi, "A Trust Based Routing Protocol for Mitigation of Sinkhole Attacks in Wireless Sensor Networks." International Journal of Information and Education Technology, Vol. 5, No. 7, July 2015.

[4]. K.Muneeswaran, "Detection of Intruders in Wireless Sensor Networks Using Anomaly." International Journal of Innovative Research in Science ,Engineering and Technology Volume 3, Special Issue 3, March 2014.

[5]. Joseph Rish Simenthy, "Advanced Intrusion Detection System for Wireless Sensor Networks." International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Special Issue 3, April 2014.

[6]. Quazi Mamun, " Anomaly Detection in Wireless Sensor Network." Journal of Networks, vol. 9, no. 11, November 2014.

[7]. P.Priyadharshini, "Trust Based Voting Scheme and Optimal Multipath Routing for Intrusion Tolerance in Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 2, February 2014, pg.255 – 260.

[8]. Swati Sharma, "Recent trend in Intrusion detection using Fuzzy-Genetic algorithm." International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 5, May 2014.

[9]. Chandra Prakash, "A Comparative Study Of Intrusion Detection System For Wireless Sensor Network." IJAFRC, Volume 1, Issue 5, May 2014.

[10]. DEEPA S, "Trust Management Schemes For Intrusion Detection Systems -A Survey." International Journal of Advanced Computational Engineering and Networking, Volume-2, Issue-8, Aug.-2014.

[11]. Mohammad Abu Alsheikh, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies, and Applications." IEEE Communications Surveys and Tutorials. 2014.

[12]. Sathyabama.B, "Energy Efficient Voting Based Intrusion Detection Techniques in Heterogeneous Wireless Sensor Network." IJCSMC, Vol. 3, Issue. 1, January 2014, pg. 374 – 380.

[13]. K.Kumaresan, " Weighted Voting based Trust Management for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks." IJAFRC, Volume 3, Issue 6, Nov 2014.

[14]. Sneha Dhage, " Intrusion Detection & Fault Tolerance in Heterogeneous Wireless Sensor Network: A Survey." International Journal of Scientific and Research Publications, Volume 4, Issue 2, February 2014.

[15]. Jaime Lloret, "Intrusion Detection Algorithm Based on Neighbor Information Against Sinkhole Attack inWireless Sensor Networks." The Computer Journal Advance Access published May 13, 2014.

[16]. Suhasini Komara, " Sinkhole Attack Detection In Hierarchical Sensor Networks." International Journal of Scientific & Engineering Research, Volume 5, Issue 9, September-2014.

[17]. Junaid Ahsenali Chaudhry, "Sinkhole Vulnerabilities in Wireless Sensor Networks." International Journal of Security and Its Applications Vol.8, No.1 (2014), pp.401-410.

[18]. Nabil Ali Alrajeh, "Secure Ant-Based Routing Protocol for Wireless Sensor Network." International Journal of Distributed Sensor Networks ,Volume 2013, Article ID 326295, 9 pages.

[19]. Udaya Suriya Rajkumar, "A Leader Based Monitoring Approach For Sinkhole Attack In Wireless Sensor Network." Journal of Computer Science 9 (9): 1106-1116, 2013.

[20]. R˘azvan Rughinis, "Adaptive Trust Management Protocol based on Intrusion Detection forWireless Sensor Networks." International Journal of Scientific & Engineering Research, Volume 1, Issue 9, September-2012.

[21]. Sibaram Khara, "K-Means Clustering In Wireless Sensor Networks." Fourth International Conference on Computational Intelligence and Communication Networks, 2012.

[22]. Shio Kumar Singh, "Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks." International Journal of Advanced Science and Technology Vol. 30, May, 2011.

[23]. Ioannis Krontiris, "Cooperative Intrusion Detection in Wireless Sensor Networks." International Journal of Distributed Sensor Networks, 2011.

[24]. Md. Safiqul Islam, "Anomaly Intrusion Detection System in Wireless Sensor Networks: Security Threats and Existing Approaches." International Journal of Advanced Science and Technology Vol. 36, November, 2011.

[25]. C. Kolias, "Swarm intelligence in intrusion detection: A survey." IJAFRC, Volume 2 Issue3, Nov 2011.

[26]. Michael Krishnan, "Intrusion Detection in Wireless Sensor Networks." ACM SENSYS, November 2010.

[27]. Marcelo H.T. Martins, "Decentralized Intrusion Detection in Wireless Sensor Networks." Q2SWinet'05, October 13, 2010.

[28]. Ioannis Krontiris, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks."International Journal of Advanced Science and Technology Vol. 36, November, 2009.

[29]. D. Sheela, "A Recent Technique to Detect Sink Hole Attacks in WSN." Journal of Computer Science 9 (9): 1106-1116, 2005.

[30]. K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats," IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs; CSE Department, vol. 1, no. 1, pp. 42–45, 2010.

[31]. H. K. D. Sarma and A. Kar, "Security Threats in Wireless Sensor Networks," in Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, Oct., pp. 243–251.

[32]. H. Ghamgin, M. S. Akhgar, and M. T. Jafari, "Attacks in Wireless Sensor Network," vol. 5, no. 7, pp. 954–960, 2011.

[33]. Padmalaya Nayak, V. Bhavani," Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 4, April 2015

[34]. M. Corporation, "Data sheet Tmote sky." Moteiv Corporation, 13-Nov-2006.